

METHOD AND SYSTEM FOR A SECURE DIGITAL DECODERABSTRACT

A method and system for securely decrypting and decoding a digital signal.

One embodiment of the present invention first receives an encrypted signal at a
5 first logical circuit. Next, this embodiment determines a broadcast encryption key
for the encrypted signal at a first location separate from the first logical circuit. For
example, the separate location where the broadcast key was determined may be
across a communication link from the first circuit where the signal is being
received. Then, the broadcast encryption key is encrypted and transferred over
10 the communication link. Next, at the first logical circuit, the encrypted broadcast
encryption key is decrypted. Therefore, the broadcast encryption key is
determined. Then, at said first logical circuit, the encrypted signal is decrypted
using the broadcast encryption key. Consequently, the encrypted signal is
decrypted without exposing the broadcast encryption key on the communication
15 link in an un-encrypted form. Another embodiment provides a method which first
generates a local encryption key. Then, the local encryption key is transferred
across a communication link to a first logical circuit and to a second logical circuit.
With the local encryption key, a digital signal at the first logical circuit is encrypted.
This encrypted signal is transferred to the second logical circuit. Thus, the signal
20 is not exposed in an un-encrypted form. Next, the second logical circuit uses the
local encryption key to decrypt the signal.